(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 June 2001 (07.06.2001)

PCT

(10) International Publication Number
WO 01/41353 A2

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number: PCT/US00/41995

(22) International Filing Date:
7 November 2000 (07.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/451,504 30 November 1999 (30.11.1999) US

(71) Applicant: SUN MICROSYSTEMS, INC. [US/US]; 901 San Antonio Road, Palo Alto, CA 94303 (US).

(72) Inventors: PERLMAN, Radia; 10 Huckleberry Lane, Acton, MA 01720-3731 (US). HANNA, Stephen; 3 Beverly Road, Bedford, MA 01730 (US).

(74) Agent: PARK, Richard; Suite 201, 508 2nd Street, Davis, CA 95616 (US).

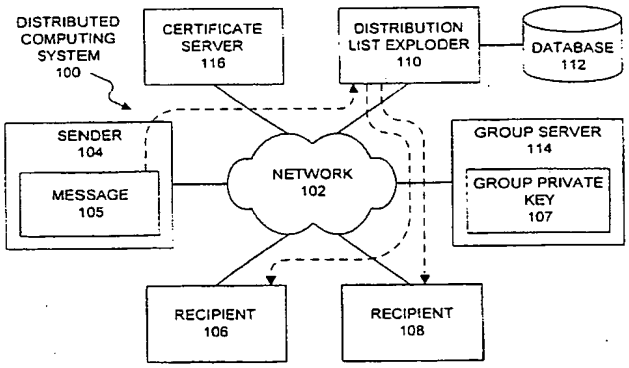
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND APPARATUS FOR SENDING ENCRYPTED ELECTRONIC MAIL THROUGH A DISTRIBUTION LIST EXPLODER



(57) Abstract: One embodiment of the present invention provides a system for sending an encrypted message through a distribution list exploder in order to forward the encrypted message to recipients on a distribution list. The system operates by encrypting the message at a sender using a message key to form an encrypted message. The system also encrypts the message key with a group public key to form an encrypted message key. The group public key is associated with a group private key to form a public key-private key pair associated with a group of valid recipients for the message. Next, the system sends the encrypted message and the encrypted message key to the distribution list exploder, and the distribution list exploder forwards the encrypted message to a plurality of recipients specified in the distribution list. After receiving the encrypted message and the encrypted message key, the recipient decrypts the encrypted message key to restore the message key. Next, the recipient decrypts the encrypted message using the message key to restore the message. In a variation on the above embodiment, the recipient decrypts the encrypted message key by sending the encrypted message key from the recipient to a group server, which holds the group private key. The group server decrypts the encrypted message key using the group private key to restore the message key, and returns the message key to the recipient in a secure manner.

WO 01/41353 A2

METHOD AND APPARATUS FOR SENDING ENCRYPTED ELECTRONIC MAIL THROUGH A DISTRIBUTION LIST EXPLODER

BACKGROUND

Field of the Invention

The present invention relates to electronic mail and encryption of data. More particularly, the present invention relates to a method and an apparatus for sending encrypted electronic mail through a distribution list exploder that forwards the electronic mail to recipients on a distribution list.

Related Art

The advent of computer networks has led to an explosion in the development of applications that facilitate rapid dissemination of information. In particular, electronic mail is becoming the predominant method for communicating textual and other non-voice information. Using electronic mail, it is just as easy to send a message to a recipient on another continent as it is to send a message to a recipient within the same building. Furthermore, an electronic mail message typically takes only a few minutes to arrive, instead of the days it takes for surface mail to snake its way along roads and through airports.

One problem with electronic mail is that it is hard to ensure that sensitive information sent through electronic mail is kept confidential. This is because an electronic mail message can potentially traverse many different computer networks and many different computer systems before it arrives at its ultimate destination. An

adversary can potentially intercept an electronic mail message at any of these intermediate points along the way.

One way to remedy this problem is to "encrypt" sensitive data using an encryption key so that only someone who possesses a corresponding decryption key can decrypt the message. (Note that for commonly used symmetric encryption mechanisms the encryption key and the decryption key are the same key.) A person sending sensitive data through electronic mail can encrypt the sensitive data using the encryption key before it is sent through email. At the other end, the recipient of the email can use the corresponding decryption key to decrypt the sensitive information.

Encryption works well for a message sent to a single recipient. However, encryption becomes more complicated for a message sent to multiple recipients. This is because encryption keys must be managed between a large number of recipients and the sender.

Conventional mail protocols, such as the Pretty Good Privacy (PGP) protocol, send mail to multiple recipients by encrypting a message with a message key (that is randomly selected for the message) to form an encrypted message. The message key is then encrypted with the public key of each of the recipients to form a set of encrypted keys. The set of encrypted keys is sent with the encrypted message to all of the recipients. Each recipient uses its private key to decrypt the encrypted message key and then uses the message key to decrypt the encrypted message.

The problem with this scheme is that the sender must know the identities of each of the recipients and must know the public key of each of the recipients. It is easier for the sender to send the message to a single machine called a distribution list exploder (DLE), which keeps track of the identities and other information for a set of recipients specified in a distribution list. This allows the DLE to forward a message to recipients specified in the distribution list. For example, in sending a message to a group of people connected with a project, a DLE can keep track of the recipients involved in the project and can route messages to the recipients. Unfortunately, existing DLE systems generally

do not support sending encrypted messages. However, there have been suggestions to provide such support. (see "NETWORK SECURITY, PRIVATE Communication in a PUBLIC World," by Charlie Kaufman, Radia Perlman and Mike Spencer, Prentice-Hall 1995, page 338)

What is needed is a method and an apparatus for sending an encrypted message to multiple recipients specified in a distribution list.

SUMMARY

One embodiment of the present invention provides a system for sending an encrypted message through a distribution list exploder in order to forward the encrypted message to recipients on a distribution list. The system operates by encrypting the message at a sender using a message key to form an encrypted message. The system also encrypts the message key with a group public key to form an encrypted message key. The group public key is associated with a group private key to form a public key-private key pair associated with a group of valid recipients for the message. Next, the system sends the encrypted message and the encrypted message key to the distribution list exploder, and the distribution list exploder forwards the encrypted message to a plurality of recipients specified in the distribution list. After receiving the encrypted message and the encrypted message key, a recipient decrypts the encrypted message key (possibly with the assistance of another machine) to restore the message key. Next, the recipient decrypts the encrypted message using the message key to restore the message.

In a variation on the above embodiment, the recipient decrypts the encrypted message key by sending the encrypted message key from the recipient to a group server, which holds the group private key. The group server decrypts the encrypted message key using the group private key to restore the message key, and returns the message key to the recipient in a secure manner.

Using a group server that is separate from the DLE to decrypt the message key makes the system more secure because the group server holds the message key while the

DLE holds the encrypted message. Hence, neither the group server nor the DLE can decrypt the message. Furthermore, by using a group server, group membership can be easily changed. Once a member is removed from the group, the former member is simply no longer allowed access to the group server.

Another advantage of using a group server is that tasks performed by the DLE, which tend to be time-consuming, can be outsourced to a high-performance third party computer system without compromising security. (This assumes that the group server functions are performed by a secure computer system, preferably under local control.)

The group server can return the message key to the recipient in a secure manner using a number of different methods. In a first method, the group server encrypts the message key using a public key belonging to the recipient to form a second encrypted message key, which is sent the recipient. The recipient restores the message key by decrypting the second encrypted message key with a corresponding recipient private key.

In a second method, the group server authenticates the recipient, verifies that the recipient is a member of the group of valid recipients for the message, and sends the message key to the recipient using a secure protocol, such as the secure sockets layer (SSL) protocol or the transport layer security (TLS) protocol.

In a third method, the recipient requests a certificate from a certificate server. If the recipient is a member of the group of valid recipients for the message, the certificate server returns the certificate (which includes a certificate public key) and a certificate private key. Next, the recipient sends the certificate to the group server. The group server encrypts the message key with the certificate public key to form a second encrypted message key and sends the second encrypted message key to the recipient. The recipient decrypts the second encrypted message key with the certificate private key to restore the message key. In a variation on the third method, the recipient generates its own private key-public key pair and sends the public key to the certificate server. The certificate server returns a certificate to the recipient, which includes the public key. In this way, the certificate server is never given access to the recipient's private key.

In a fourth method, the group server encrypts the message using a group key, which is a symmetric key that is shared among members of a group of valid recipients, to form a second encrypted message key and sends the second encrypted message key to the recipient. The recipient decrypts the second encrypted message key using the shared group key to restore the message key.

In another variation on the above embodiment, instead of going to the group server, the recipient possesses the group private key and uses the group private key to decrypt the encrypted message key.

In one embodiment of the present invention, the distribution list exploder sends the encrypted message key to a group server which holds the group private key. The group server decrypts the encrypted message key using the group private key to restore the message key. Next, the group server encrypts the message key with a secret key known to the group of valid recipients for the message to form a second encrypted message key. The group server sends the second encrypted message key to the distribution list exploder. The distribution list exploder forwards the encrypted message and the second encrypted message key to the plurality of recipients. One advantage of this embodiment is that it does not require the group server to interact with all recipients, which can greatly reduce the burden on the group server.

BRIEF DESCRIPTION OF THE FIGURES

FIG. 1 illustrates a distributed computer system in accordance with an embodiment of the present invention.

FIG. 2 illustrates portions of the encryption and decryption process in accordance with an embodiment of the present invention.

FIG. 3 illustrates how a group server is involved in the decryption process in accordance with an embodiment of the present invention.

FIG. 4A is a portion of a flow chart illustrating the encryption process and the decryption process in accordance with an embodiment of the present invention.

FIG. 4B is another portion of a flow chart illustrating the encryption process and the decryption process in accordance with an embodiment of the present invention.

FIG. 4C is yet another portion of a flow chart illustrating the encryption process and the decryption process in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION

The following description is presented to enable any person skilled in the art to make and use the invention, and is provided in the context of a particular application and its requirements. Various modifications to the disclosed embodiments will be readily apparent to those skilled in the art, and the general principles defined herein may be applied to other embodiments and applications without departing from the spirit and scope of the present invention. Thus, the present invention is not intended to be limited to the embodiments shown, but is to be accorded the widest scope consistent with the principles and features disclosed herein.

The data structures and code described in this detailed description are typically stored on a computer readable storage medium, which may be any device or medium that can store code and/or data for use by a computer system. This includes, but is not limited to, magnetic and optical storage devices such as disk drives, magnetic tape, CDs (compact discs) and DVDs (digital video discs), and computer instruction signals embodied in a transmission medium (with or without a carrier wave upon which the signals are modulated). For example, the transmission medium may include a communications network, such as the Internet.

Distributed Computer System

FIG. 1 illustrates distributed computer system 100 in accordance with an embodiment of the present invention. The components of distributed computer system 100 are coupled together by a network 102. Network 102 can include any type of wire or wireless communication channel capable of coupling together computing nodes. This

includes, but is not limited to, a local area network, a wide area network, or a combination of networks. In one embodiment of the present invention, network 102 includes the Internet.

Distributed computer system 100 also includes a number of computer systems that send and receive electronic mail (email), including sender 104 and recipients 106 and 108. Sender 104 can include any type of computing system that can send an email message, while recipients 106 and 108 can include any type of computing systems that can receive an email message.

Distributed computer system 100 includes a number of servers that can be involved in the process of encrypting and forwarding email messages. These servers include certificate server 116, group server 114 and distribution list exploder (DLE) 110.

Certificate server 116 can include any type of machine that can issue a digital certificate to a valid recipient for an email message. For purposes of this detailed disclosure, a certificate is a signed electronic document that certifies that something is true. A certificate typically indicates that someone has ownership of a public key-private key pair. For purposes of the present invention, a certificate can indicate that the holder of the certificate is a member of a group of valid recipients for a message. A certificate may include the identity of a signing authority as well as a digital signature produced with a private key (that can be validated with a corresponding public key). For example, one certificate format is defined under the X.509 standard.

Distribution list exploder (DLE) 110 can include any type of machine that can forward an email message to a group of recipients specified in a distribution list. Note that DLE 110 is coupled to database 112. Database 112 stores identification information for members of a distribution list, and can also store encryption information, such as public keys, for members of the distribution list.

Group server 114 can include any type of server that can assist in the decryption process of an email message. In one embodiment of the present invention, group server

114 holds a group private key 302, which can be used to decrypt encrypted messages sent to a group of recipients specified on a distribution list.

The system illustrated in FIG. 1 operates generally as follows. Sender 104 sends message 105 in encrypted form to DLE 110. DLE 110 looks up recipients within a corresponding distribution list for message 105 stored in database 112. DLE 110 then forwards message 105 in encrypted form to recipients 106 and 108 specified in the distribution list.

Once recipients 106 and 108 receive message 105 in encrypted form, they can access group server 114 for help in decrypting message 105. In doing so, recipients 106 and 108 can make requests to certificate server 116 to receive certificates that can be presented to group server 114 to certify that they are valid recipients for message 105.

Encryption and Decryption

FIG. 2 illustrates portions of the encryption and decryption process in accordance with an embodiment of the present invention. Sender 104 encrypts message 105 with message key 204 to produce encrypted message 206. Message key 204 can be a per-message key that is randomly generated for message 105. Message key 204 is itself encrypted with group public key 107 to form encrypted message key 210. Group public key 107 is part of a public key-private key pair that is associated with a group of valid recipients for message 105. A data item that is encrypted with group public key 107 can be decrypted with corresponding group private key 302. Finally, encrypted message 206 is appended to encrypted message key 210 to form bundle 212, and bundle 212 is sent through DLE 110 to recipients 106 and 108.

At recipient 106, encrypted message key 210 is decrypted to restore message key 204. Note that this decryption process may involve communications with group server 114 as is described in more detail with reference to FIG. 3 below. Message key 204 is then used to decrypt encrypted message 206 to restore message 105. Note that the

encryption process used for message 105 is symmetric, which means that the same message key 204 can be used to both encrypt and decrypt message 105.

Group Server

FIG. 3 illustrates how group server 114 can be involved in the decryption process in accordance with an embodiment of the present invention. FIG. 3 illustrates in more detail how decryption module 214 within recipient 106 operates. Encrypted message key 210 is sent to group server 114, which holds group private key 302. Group server 114 decrypts encrypted message key 210 using group private key 302 to restore message key 204. In order to securely send message key 204 back to recipient 106, message key 204 is again encrypted to form encrypted message key 308.

This encryption process can happen in a number of ways. It can involve using a public key 312 belonging to recipient 106. It can involve using a group secret key 314 known only to a group of valid recipients for message 105. It can involve using a secure protocol session key, such as a secure sockets layer (SSL) session key 316. Or, it can involve using a certificate public key 317 associated with a certificate issued by certificate server 116. Encrypted message key 308 is then sent to recipient 106. Next, recipient 106 decrypts encrypted message key 308 to restore message key 204.

Note that it is possible for DLE 110 to handle both the forwarding of message 105 and the decrypting of encrypted message key 210. However, this requires DLE 110 to have access to group private key 302, which allows DLE 110 to decrypt encrypted message 206 if it wants to. This can greatly compromise system security if DLE 110 cannot be completely trusted.

On the other hand, if group private key 302 is held by group server 114, DLE 110 is not able decrypt encrypted message 206. At the same time, group server 114 does not possess encrypted message 206, so group server 114 cannot decrypt encrypted message 206 either. Hence, in this case neither DLE 110 nor group server 114 needs to be completely trusted.

Encryption Process and Decryption Process

FIG. 4A is a portion of a flow chart illustrating the encryption process and the decryption process in accordance with an embodiment of the present invention. The system starts by encrypting message 105 with message key 204 to form encrypted message 206 within sender 104 (step 402). Message key 204 is itself encrypted with group public key 107 to form encrypted message key 210 (step 404). Next, encrypted message 206 and encrypted message key 210 are sent to DLE 110 (step 406).

At this point there are two different options (A and B) associated with two different embodiments of the present invention. Under option A, DLE 110 forwards encrypted message 206 and encrypted message key 210 to recipients 106 and 108 specified in a distribution list for the message (step 408). In doing so, DLE 110 looks up information related to recipients 106 and 108 in database 112 in FIG. 1.

At this point there are two additional options (C and D) associated with different embodiments of the present invention. Under option C, a recipient 106, who receives encrypted message 206 and encrypted message key 210, decrypts encrypted message key 210 using group private key 302 to restore message key 204 (step 410). Recipient 106 then decrypts encrypted message 206 to restore message 105 using message key 204 (step 412). At this point, recipient 106 has the decrypted message 105 and the process is complete. However, note that this embodiment requires all recipients of message 105 to know group private key 302. This can create administrative problems if the group of valid recipients changes over time. New public key-private key pairs must continually be generated and distributed as the group changes.

In order to remedy this problem, option D uses group server 114 to hold group private key 302. After recipient 106 receives encrypted message 206 and encrypted message key 210, recipient 106 sends encrypted message key 210 to group server 114 (step 414). Group server 114 uses group private key 302 to decrypt encrypted message key 210 to restore message key 204 (step 416).

At this point there are three options (E, F and G) associated with different methods for returning message key 204 to recipient 106 securely. Under option E, group server 114 encrypts message key 204 using a public key belonging to recipient 106 to form encrypted message key 308 (step 418). Encrypted message key 308 is then sent to recipient 106 (step 420). Recipient 106 decrypts encrypted message key 308 using a corresponding private key belonging to recipient 106 to restore message key 204 (step 422), and then decrypts encrypted message 206 using message key 204 (step 412). At this point, recipient 106 has the decrypted message 105 and the process is complete.

FIG. 4B illustrates what happens during options F and G in accordance with other embodiments of the present invention. Under option F, group server 114 authenticates the identity of recipient 106 (step 440), and verifies that recipient 106 is a member of a group of valid recipients for message 105 (step 442. Next, group server 114 sends message key 204 to recipient 106 using a secure protocol, such as the SSL protocol or the TLS protocol (step 444). Note that using these protocols inherently involves encrypting and decrypting message key 204 with a secure protocol session key. Next, recipient 106 decrypts encrypted message 206 using message key 204 to restore message 105 (step 446). At this point, recipient 106 has the decrypted message 105 and the process is complete.

Under option G, recipient 106 requests a certificate from certificate server 116 (step 450). If recipient 106 can successfully authenticate itself to certificate server 116, and if recipient 106 is a member of a group of valid recipients for message 105, then recipient 106 receives a certificate and an associated private key from certificate server 116 (step 452). Recipient 106 then sends the certificate to group server 114 (step 454). Group server 114 encrypts message key 204 with certificate public key 317 to form encrypted message key 308 (step 456). Encrypted message key 308 is then sent to recipient 106 (step 458). Recipient 106 decrypts encrypted message key 308 using a corresponding certificate private key to restore message key 204 (step 460), and then decrypts encrypted message 206 using message key 204 (step 446). At this point,

recipient 106 has the decrypted message 105 and the process is complete. Note that the embodiment outlined under option G allows for recipient 106 to anonymously request message key 204 without revealing its identity to group server 114.

Under option G, note that the recipient can alternatively request a certificate in advance, and can use the certificate for multiple messages. Also note that, as mentioned previously, the recipient can alternatively generate its own private key-public key pair, and can send the public key to the certificate server. The certificate server returns a certificate to the recipient, which includes the public key. In this way, the certificate server never has access to the recipient's private key.

FIG. 4C illustrates what happens during option B in accordance with an embodiment of the present invention. After DLE 110 receives encrypted message 206 and encrypted message key 210, DLE 110 sends encrypted message key 210 to group server 114 (step 424). Next, group server 114 decrypts encrypted message key 210 using group private key 302 to restore message key 204 (step 426). Group server 114 then encrypts message key 204 with group secret key 314 to form encrypted message key 308 (step 428), and sends encrypted message key 308 to DLE 110 (step 430). DLE 110 forwards encrypted message 206 and encrypted message key 308 to recipients 106 and 108 specified in the distribution list (step 432). Recipient 106 decrypts encrypted message key 308 using group secret key 314 to restore message key 204 (step 434). Next, recipient 106 decrypts encrypted message 206 using message key 204 to restore message 105 (step 436). At this point, recipient 106 has the decrypted message 105 and the process is complete.

Note that the embodiment associated with option B simply replaces encrypted message key 210 (which is encrypted with group public key 107) with encrypted message key 308 (which is encrypted using group secret key 314). Under option B, recipients 106 and 108 are presumed to know group secret key 314 instead of group private key 302. This is advantageous because if group membership changes, propagating a new group public key to all potential senders can be a time-consuming and error-prone task. In

contrast, propagating a new group secret key to members of a group of valid recipients is an easier task.

The foregoing descriptions of embodiments of the invention have been presented for purposes of illustration and description only. They are not intended to be exhaustive or to limit the invention to the forms disclosed. Accordingly, many modifications and variations will be apparent to practitioners skilled in the art. Additionally, the above disclosure is not intended to limit the invention. The scope of the invention is defined by the appended claims.

What Is Claimed Is:

1. A method for sending a message that is encrypted through a distribution list exploder that forwards the message to recipients on a distribution list, comprising:

encrypting the message at a sender using a message key to form an encrypted message, the message key being randomly selected for the message;

encrypting the message key with a group public key to form an encrypted message key, the group public key being associated with a group private key to form a public key-private key pair associated with a group of valid recipients for the message;

sending the encrypted message and the encrypted message key to the distribution list exploder, the distribution list exploder being configured to forward the encrypted message to a plurality of recipients specified in the distribution list;

forwarding the encrypted message and the encrypted message key from the distribution list exploder to the plurality of recipients;

receiving the encrypted message and the encrypted message key at a recipient from the plurality of recipients;

sending the encrypted message key from the recipient to a group server, the group server possessing the group private key;

decrypting the encrypted message key at the group server using the group private key to restore the message key;

communicating the message key to the recipient in a secure manner;

decrypting the encrypted message at the recipient using the message key to restore the message.

2. A method for sending a message that is encrypted through a distribution list exploder that forwards the message to recipients on a distribution list, comprising:

encrypting the message at a sender using a message key to form an encrypted message;

encrypting the message key with a group public key to form an encrypted message key, the group public key being associated with a group private key to form a public key-private key pair associated with a group of valid recipients for the message; and

sending the encrypted message and the encrypted message key to the distribution list exploder, the distribution list exploder being configured to forward the encrypted message to a plurality of recipients specified in the distribution list.

3. The method of claim 2, further comprising:

forwarding the encrypted message and the encrypted message key from the distribution list exploder to the plurality of recipients;

decrypting the encrypted message key at a recipient from the plurality of recipients to restore the message key; and

decrypting the encrypted message at the recipient using the message key to restore the message.

4. The method of claim 3, wherein decrypting the encrypted message key includes using the group private key to decrypt the encrypted message key, the group private key being known by members of the group of valid recipients for the message.

5. The method of claim 3, wherein decrypting the encrypted message key at the recipient further comprises:

sending the encrypted message key from the recipient to a group server, the group server possessing the group private key;

decrypting the encrypted message key at the group server using the group private key to restore the message key; and

communicating the message key to the recipient in a secure manner.

6. The method of claim 5, wherein communicating the message key to the recipient in a secure manner comprises:

encrypting the message key at the group server using a recipient public key belonging to the recipient to form a second encrypted message key, the recipient public key being associated with a recipient private key to form a public key-private key pair associated with the recipient;

sending the second encrypted message key to the recipient; and

at the recipient, decrypting the second encrypted message key with the recipient private key to restore the message key.

7. The method of claim 5, wherein communicating the message key to the recipient in a secure manner comprises:

authenticating the recipient;

verifying that the recipient is a member of the group of valid recipients for the message; and

sending the message key to the recipient using a secure protocol.

8. The method of claim 7, wherein the secure protocol includes one of, the transport layer security (TLS) protocol and the secure sockets layer (SSL) protocol.

9. The method of claim 5, wherein communicating the message key to the recipient in a secure manner comprises:

making a request from the recipient to a certificate server for a certificate, the certificate including a certificate public key, the certificate public key being associated with a certificate private key to form a public key-private key pair;

sending the certificate from the certificate server to the recipient only if the recipient is a member of the group of valid recipients for the message;

sending the certificate from the recipient to the group server;

encrypting the message key with the certificate public key to form a second encrypted message key;

sending the second encrypted message key to the recipient; and

at the recipient, decrypting the second encrypted message key with the certificate private key to restore the message key.

10. The method of claim 5, wherein communicating the message key to the recipient in a secure manner comprises:

encrypting the message key at the group server using a group secret key to form a second encrypted message key, the group secret key being a symmetric key known to the group of valid recipients;

sending the second encrypted message key to the recipient; and

at the recipient, decrypting the second encrypted message key with the group secret key to restore the message key.

11. The method of claim 2, further comprising:

sending the encrypted message key from the distribution list exploder to a group server, the group server possessing the group private key;

decrypting the encrypted message key at the group server using the group private key to restore the message key;

encrypting the message key with a secret key to form a second encrypted message key, the secret key being known to the group of valid recipients for the message;

wherein encrypting the message key with the secret key involves using a symmetric encryption mechanism so that the second encrypted message key can be decrypted using the secret key;

sending the second encrypted message key from the group server to the distribution list exploder; and

forwarding the encrypted message and the second encrypted message key from the distribution list exploder to the plurality of recipients.

12. The method claim 11, further comprising:

decrypting the encrypted message key at a recipient from the plurality of recipients using the secret key to restore the message key; and

decrypting the encrypted message with the message key to restore the message at the recipient.

13. The method of claim 2, further comprising:

decrypting the encrypted message key at the distribution list exploder using the group private key to restore the message key;

encrypting the message key with a secret key to form a second encrypted message key, the secret key being known to the group of valid recipients for the message;

wherein encrypting the message key with the secret key involves using a symmetric encryption mechanism so that the second encrypted message key can be decrypted using the secret key; and

sending the encrypted message and the second encrypted message key from the distribution list exploder to the plurality of recipients.

14. A computer readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for sending a message that is encrypted through a distribution list exploder that forwards the message to recipients on a distribution list, comprising:

encrypting the message at a sender using a message key to form an encrypted message;

encrypting the message key with a group public key to form an encrypted message key, the group public key being associated with a group private key to form a public key-private key pair associated with a group of valid recipients for the message; and

sending the encrypted message and the encrypted message key to the distribution list exploder, the distribution list exploder being configured to forward the encrypted message to a plurality of recipients specified in the distribution list.

15. An apparatus that facilitates sending a message that is encrypted through a distribution list exploder that forwards the message to recipients on a distribution list, comprising:

an encryption mechanism, that is configured to,

encrypt the message using a message key to form an encrypted message, and to

encrypt the message key with a group public key to form an encrypted message key, the group public key being associated with a group private key to form a public key-private key pair associated with a group of valid recipients for the message; and

a sending mechanism that is configured to send the encrypted message and the encrypted message key to the distribution list exploder, the distribution list exploder being configured to forward the encrypted message to a plurality of recipients specified in the distribution list.

16. The apparatus of claim 15, further comprising:

a distribution mechanism within the distribution list exploder that is configured to forward the encrypted message and the encrypted message key from the distribution list exploder to the plurality of recipients;

a first decryption mechanism at a recipient from the group of recipients that is configured to decrypt the encrypted message key to restore the message key; and

a second decryption mechanism at the recipient that is configured to decrypt the encrypted message using the message key to restore the message.

17. The apparatus of claim 16, wherein the first decryption mechanism is configured to use the group private key to decrypt the encrypted message key, the group private key being known by members of the group.

18. The apparatus of claim 16, wherein the first decryption mechanism further comprises:

a second sending mechanism that is configured to send the encrypted message key from the recipient to a group server, the group server possessing the group private key;

a third decryption mechanism within the group server that is configured to decrypt the encrypted message key using the group private key to restore the message key;

a communication mechanism that is configured to send the message key from the group server to the recipient in a secure manner.

19. The apparatus of claim 18, wherein the communication mechanism further comprises:

a third encryption mechanism that is configured to encrypt the message key using a recipient public key belonging to the recipient to form a second encrypted message key, the recipient public key being associated with a recipient private key to form a public key-private key pair associated with the recipient;

a third sending mechanism that is configured to send the second encrypted message key to the recipient; and

a fourth decryption mechanism within the recipient that is configured to decrypt the second encrypted message key with the recipient private key to restore the message key.

20. The apparatus of claim 18, wherein the communication mechanism further comprises:

an authentication mechanism within the group server that is configured to authenticate the recipient;

a verification mechanism within the group server that is configured to verify that the recipient is a member of the group of valid recipients for the message; and

a secure sending mechanism that is configured to send the message key to the recipient using a secure protocol.

21. The apparatus of claim 20, wherein the secure protocol includes one of, the transport layer security (TLS) protocol and the secure sockets layer (SSL) protocol.

22. The apparatus of claim 18, wherein the communication mechanism further comprises:

a requesting mechanism that is configured to make a request from the recipient to a certificate server for a certificate, the certificate including a certificate public key, the certificate public key being associated with a certificate private key to form a public key-private key pair;

a receiving mechanism within the recipient that is configured to receive the certificate from the certificate server;

wherein the second sending mechanism is further configured to send the certificate from the recipient to the group server;

a second encryption mechanism within the group server that is configured to encrypt the message key with the certificate public key to form a second encrypted message key;

a third sending mechanism that is configured to send the second encrypted message key to the recipient; and

wherein the second decryption mechanism is further configured to decrypt the second encrypted message key with the certificate private key to restore the message key.

23. The apparatus of claim 18, wherein the communication mechanism further comprises:

a third encryption mechanism that is configured to encrypt the message key using a group secret key, the group secret key being a symmetric key known to the group of valid recipients;

a third sending mechanism that is configured to send the second encrypted message key to the recipient; and

a fourth decryption mechanism within the recipient that is configured to decrypt the second encrypted message key with the group secret key to restore the message key.

24. The apparatus of claim 15, further comprising:

a second sending mechanism that is configured to send the encrypted message key from the distribution list exploder to a group server, the group server possessing the group private key;

a decryption mechanism within the group server that is configured to decrypt the encrypted message key using the group private key to restore the message key;

a second encryption mechanism within the group server that is configured to encrypt the message key with a secret key to form a second encrypted message key, the secret key being known to the group of valid recipients for the message;

wherein the second encryption mechanism includes a symmetric encryption mechanism so that the second encrypted message key can be decrypted using the secret key;

a third sending mechanism within the group server that is configured to send the second encrypted message key to the distribution list exploder; and

a distribution mechanism within the distribution list exploder that is configured to forward the encrypted message and the second encrypted message key to the plurality of recipients.

25. A method for receiving a message that is encrypted through a distribution list exploder that forwards the message to recipients on a distribution list, comprising:

receiving an encrypted message and an encrypted message key from the distribution list exploder at a recipient;

wherein the encrypted message contains the message that is encrypted using a message key;

wherein the encrypted message key contains the message key that is encrypted using a group public key, the group public key being associated with a group private key to form a public key-private key pair associated with a group of valid recipients for the message;

sending the encrypted message key from the recipient to a group server, the group server possessing the group private key;

allowing the group server to decrypt the encrypted message key using the group private key to restore the message key; and

receiving the message key from the group server in a secure manner;

decrypting the encrypted message key at the recipient to restore the message key; and

decrypting the encrypted message at the recipient using the message key to restore the message.

26. The method of claim 25, wherein receiving the message key from the group server in the secure manner comprises:

allowing the group server to encrypt the message key using a recipient public key belonging to the recipient to form a second encrypted message key, the recipient public

key being associated with a recipient private key to form a public key-private key pair associated with the recipient;

receiving the second encrypted message key from the group server; and

decrypting the second encrypted message key with the recipient private key to restore the message key.

27. The method of claim 25, wherein receiving the message key from the group server in the secure manner comprises:

authenticating the recipient to the group server;

allowing the group server to verify that the recipient is a member of the group of valid recipients for the message; and

receiving the message key from the group server at the recipient using a secure protocol.

28. The method of claim 27, wherein the secure protocol includes one of, the transport layer security (TLS) protocol and the secure sockets layer (SSL) protocol.

29. The method of claim 25, wherein receiving the message key from the group server in the secure manner comprises:

making a request from the recipient to a certificate server for a certificate, the certificate including a certificate public key, the certificate public key being associated with a certificate private key to form a public key-private key pair;

receiving the certificate from the certificate server only if the recipient is a member of the group of valid recipients for the message;

sending the certificate from the recipient to the group server;

allowing the group server to encrypt the message key with the certificate public key to form a second encrypted message key;

receiving the second encrypted message key at the recipient; and

decrypting the second encrypted message key with the certificate private key to restore the message key.

30. The method of claim 25, wherein receiving the message key from the group server in the secure manner comprises:

allowing the group server to encrypt the message key using a group secret key to form a second encrypted message key, the group secret key being a symmetric key known to the group of valid recipients;

receiving the second encrypted message key at the recipient; and

decrypting the second encrypted message key with the group secret key to restore the message key.

31. A method for sending a message that is encrypted through a distribution list exploder that forwards the message to recipients on a distribution list, comprising:

receiving an encrypted message and an encrypted message key from a sender at the distribution list exploder;

wherein the encrypted message contains the message that is encrypted using a message key;

wherein the encrypted message key contains the message key that is encrypted using a group public key, the group public key being associated with a group private key to form a public key-private key pair associated with a group of valid recipients for the message;

sending the encrypted message key from the distribution list exploder to a group server, the group server possessing the group private key;

allowing the group server to decrypt the encrypted message key using the group private key to restore the message key;

allowing the group server to encrypt the message key with a secret key to form a second encrypted message key, the secret key being known to the group of valid recipients for the message;

wherein encrypting the message key with the secret key involves using a symmetric encryption mechanism so that the second encrypted message key can be decrypted using the secret key;

receiving the second encrypted message key from the group server to the distribution list exploder; and

forwarding the encrypted message and the second encrypted message key from the distribution list exploder to a plurality of recipients.

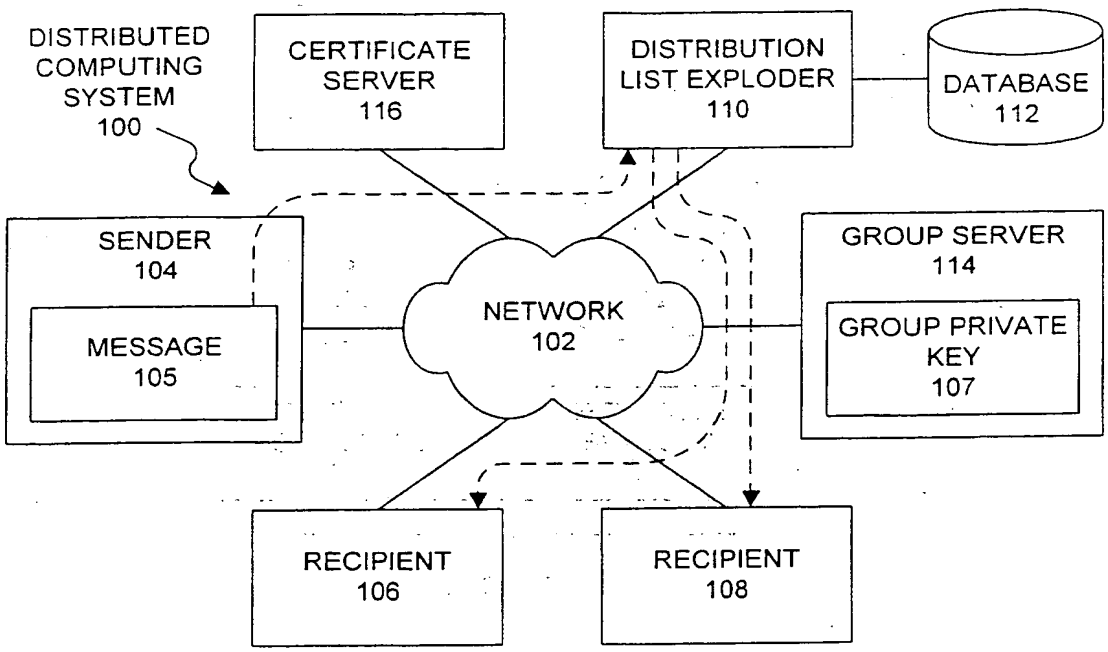

DISTRIBUTED COMPUTING SYSTEM 100
CERTIFICATE SERVER 116
DISTRIBUTION LIST EXPLODER 110
DATABASE 112
SENDER 104
MESSAGE 105
NETWORK 102
GROUP SERVER 114
GROUP PRIVATE KEY 107
RECIPIENT 106
RECIPIENT 108

FIG. 1

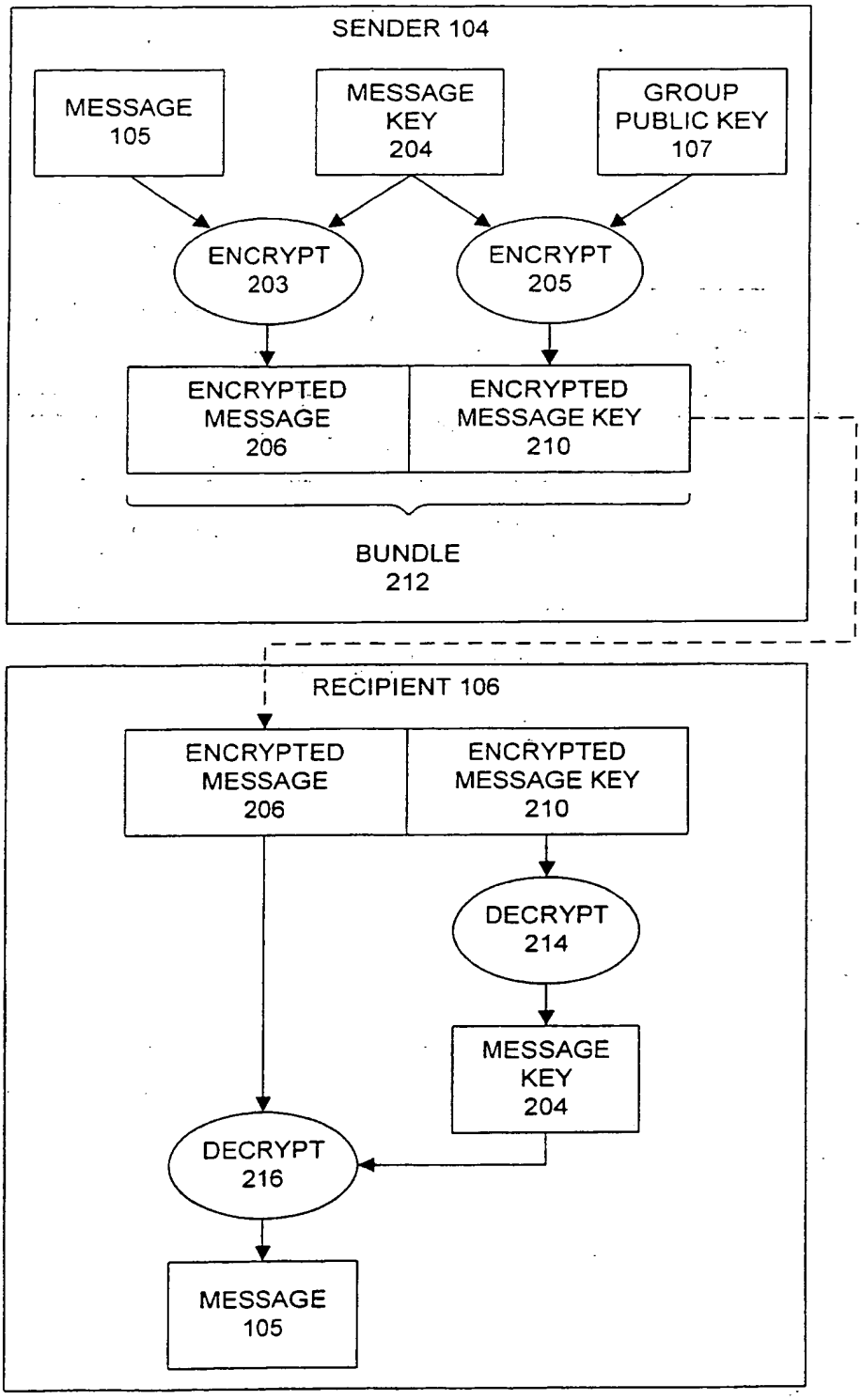

SENDER 104
MESSAGE 105
MESSAGE KEY 204
GROUP PUBLIC KEY 107
ENCRYPT 203
ENCRYPT 205
ENCRYPTED MESSAGE 206
ENCRYPTED MESSAGE KEY 210
BUNDLE 212
RECIPIENT 106
ENCRYPTED MESSAGE 206
ENCRYPTED MESSAGE KEY 210
DECRYPT 214
MESSAGE KEY 204
DECRYPT 216
MESSAGE 105

FIG. 2

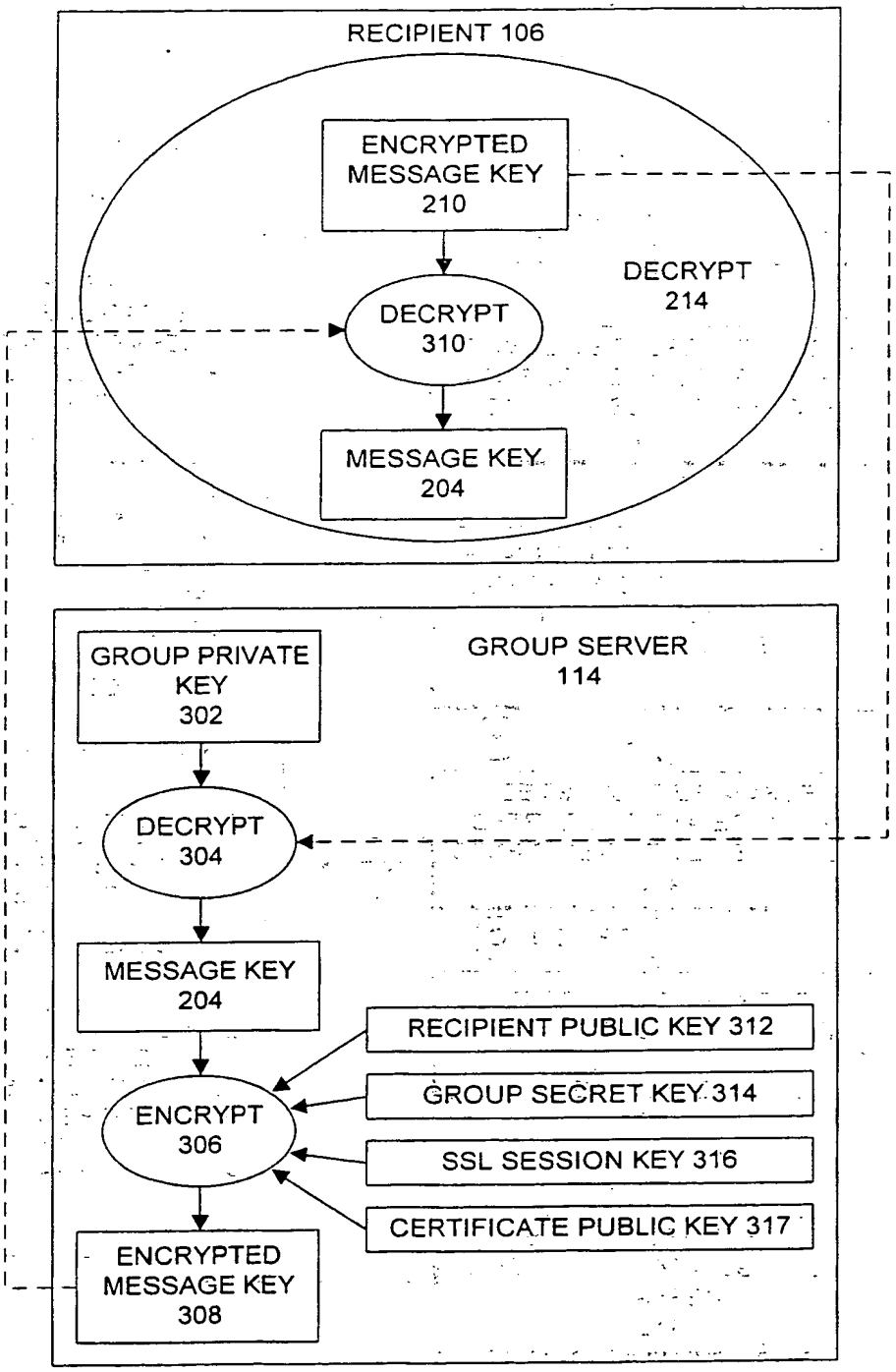

RECIPIENT 106
ENCRYPTED MESSAGE KEY 210
DECRYPT 214
DECRYPT 310
MESSAGE KEY 204
GROUP PRIVATE KEY 302
GROUP SERVER 114
DECRYPT 304
MESSAGE KEY 204
RECIPIENT PUBLIC KEY 312
GROUP SECRET KEY 314
ENCRYPT 306
SSL SESSION KEY 316
CERTIFICATE PUBLIC KEY 317
ENCRYPTED MESSAGE KEY 308

FIG. 3

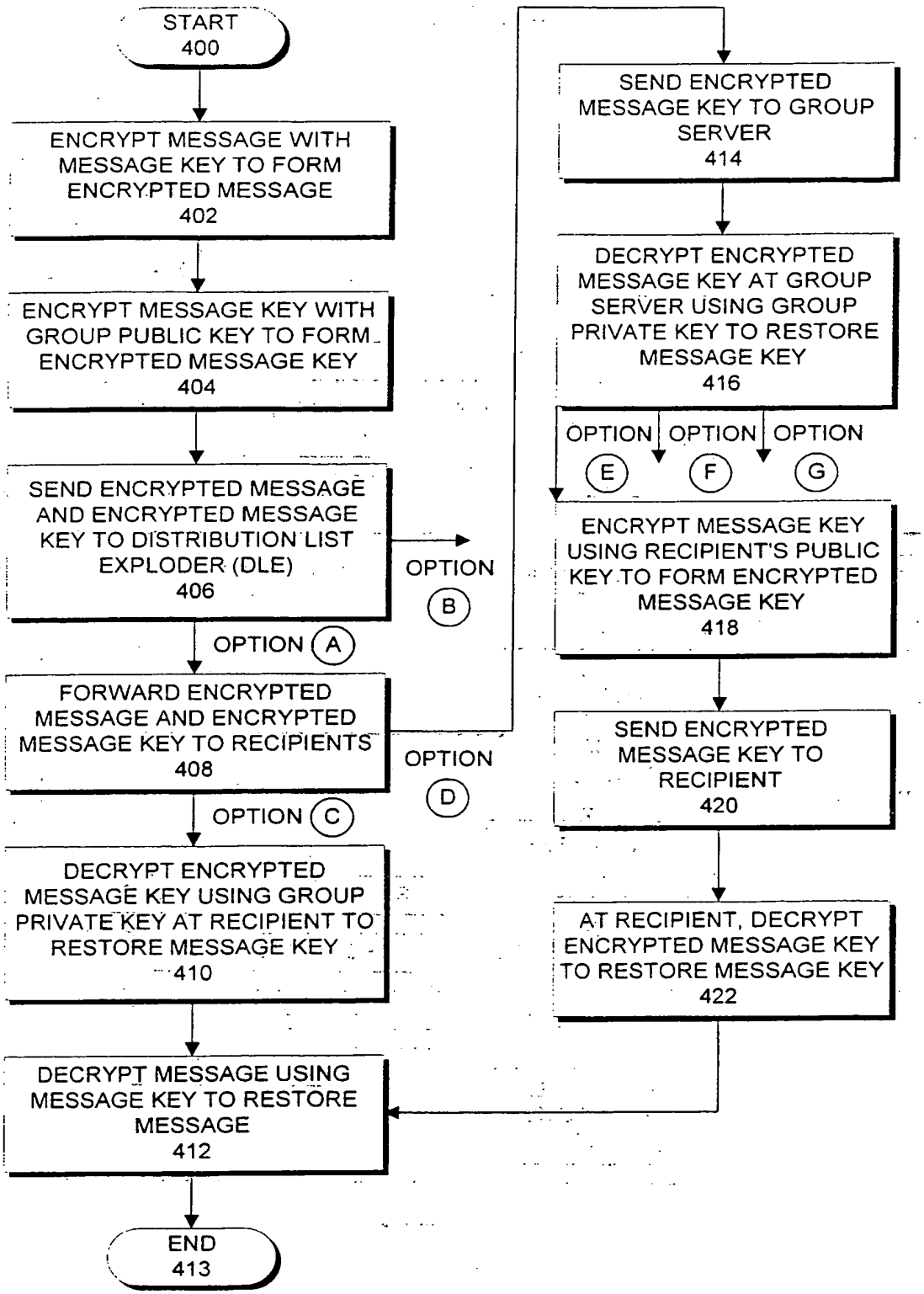

START
400
ENCRYPT MESSAGE WITH MESSAGE KEY TO FORM ENCRYPTED MESSAGE
402
ENCRYPT MESSAGE KEY WITH GROUP PUBLIC KEY TO FORM ENCRYPTED MESSAGE KEY
404
SEND ENCRYPTED MESSAGE AND ENCRYPTED MESSAGE KEY TO DISTRIBUTION LIST EXPLODER (DLE)
406
OPTION B
OPTION A
FORWARD ENCRYPTED MESSAGE AND ENCRYPTED MESSAGE KEY TO RECIPIENTS
408
OPTION D
OPTION C
DECRYPT ENCRYPTED MESSAGE KEY USING GROUP PRIVATE KEY AT RECIPIENT TO RESTORE MESSAGE KEY
410
DECRYPT MESSAGE USING MESSAGE KEY TO RESTORE MESSAGE
412
END
413
SEND ENCRYPTED MESSAGE KEY TO GROUP SERVER
414
DECRYPT ENCRYPTED MESSAGE KEY AT GROUP SERVER USING GROUP PRIVATE KEY TO RESTORE MESSAGE KEY
416
OPTION E
OPTION F
OPTION G
ENCRYPT MESSAGE KEY USING RECIPIENT'S PUBLIC KEY TO FORM ENCRYPTED MESSAGE KEY
418
SEND ENCRYPTED MESSAGE KEY TO RECIPIENT
420
AT RECIPIENT, DECRYPT ENCRYPTED MESSAGE KEY TO RESTORE MESSAGE KEY
422

FIG. 4A

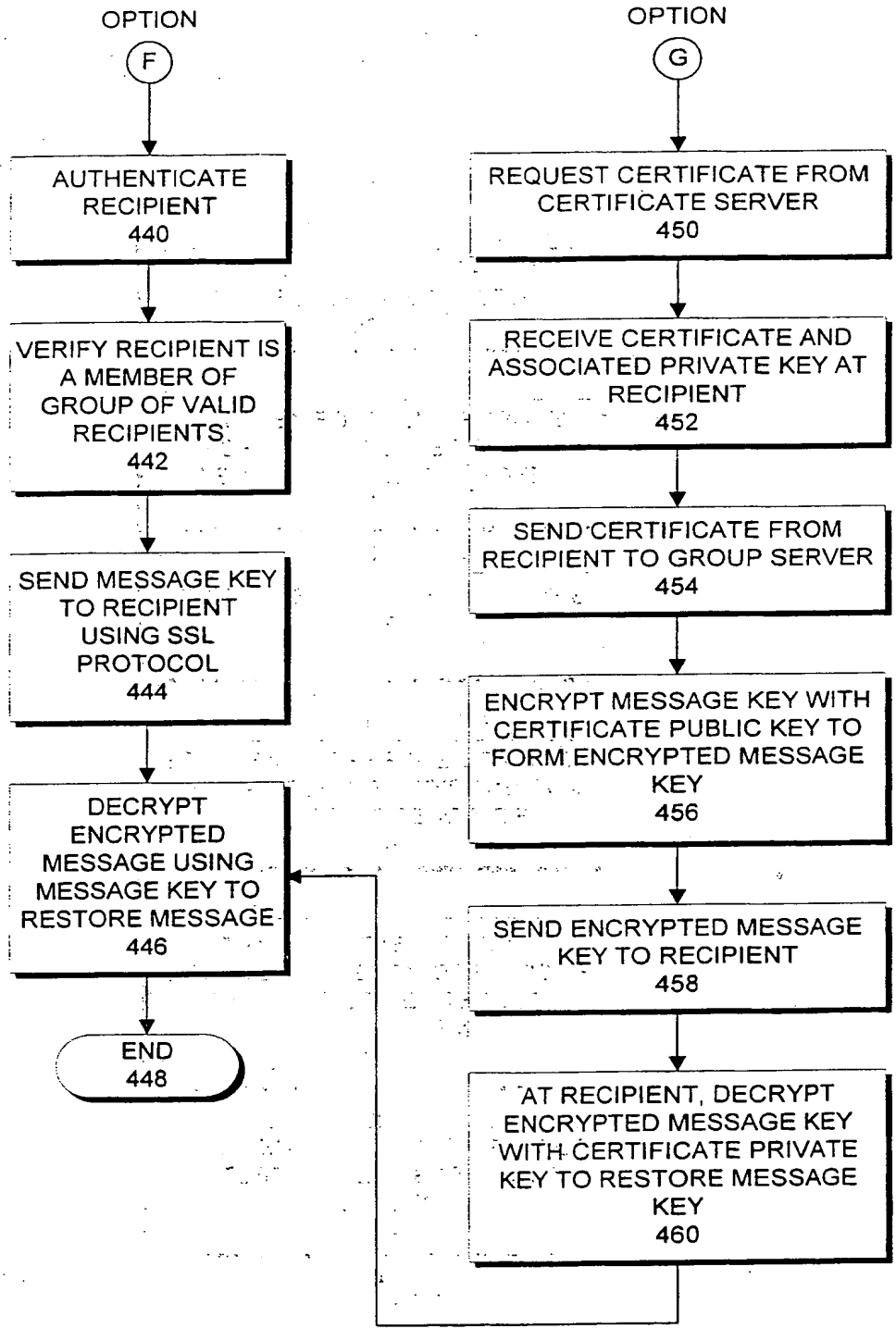

OPTION
F
AUTHENTICATE RECIPIENT 440
VERIFY RECIPIENT IS A MEMBER OF GROUP OF VALID RECIPIENTS 442
SEND MESSAGE KEY TO RECIPIENT USING SSL PROTOCOL 444
DECRYPT ENCRYPTED MESSAGE USING MESSAGE KEY TO RESTORE MESSAGE 446
END 448
OPTION
G
REQUEST CERTIFICATE FROM CERTIFICATE SERVER 450
RECEIVE CERTIFICATE AND ASSOCIATED PRIVATE KEY AT RECIPIENT 452
SEND CERTIFICATE FROM RECIPIENT TO GROUP SERVER 454
ENCRYPT MESSAGE KEY WITH CERTIFICATE PUBLIC KEY TO FORM ENCRYPTED MESSAGE KEY 456
SEND ENCRYPTED MESSAGE KEY TO RECIPIENT 458
AT RECIPIENT, DECRYPT ENCRYPTED MESSAGE KEY WITH CERTIFICATE PRIVATE KEY TO RESTORE MESSAGE KEY 460

FIG. 4B

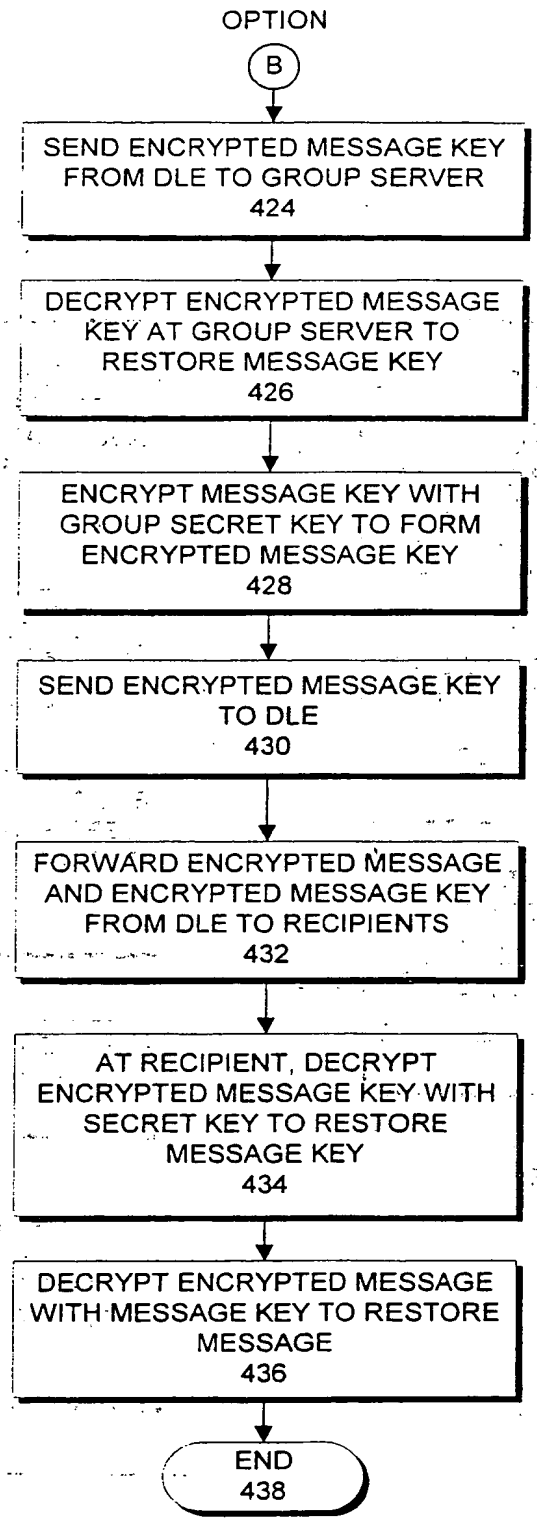

OPTION
B
SEND ENCRYPTED MESSAGE KEY FROM DLE TO GROUP SERVER
424
DECRYPT ENCRYPTED MESSAGE KEY AT GROUP SERVER TO RESTORE MESSAGE KEY
426
ENCRYPT MESSAGE KEY WITH GROUP SECRET KEY TO FORM ENCRYPTED MESSAGE KEY
428
SEND ENCRYPTED MESSAGE KEY TO DLE
430
FORWARD ENCRYPTED MESSAGE AND ENCRYPTED MESSAGE KEY FROM DLE TO RECIPIENTS
432
AT RECIPIENT, DECRYPT ENCRYPTED MESSAGE KEY WITH SECRET KEY TO RESTORE MESSAGE KEY
434
DECRYPT ENCRYPTED MESSAGE WITH MESSAGE KEY TO RESTORE MESSAGE
436
END
438

FIG. 4C

This Page Blank (uspto)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 June 2001 (07.06.2001)

PCT

(10) International Publication Number
WO 01/41353 A3

(51) International Patent Classification⁷: H04L 9/08, 29/06

(21) International Application Number: PCT/US00/41995

(22) International Filing Date:
7 November 2000 (07.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/451,504 30 November 1999 (30.11.1999) US

(71) Applicant: SUN MICROSYSTEMS, INC. [US/US]; 901 San Antonio Road, Palo Alto, CA 94303 (US).

(72) Inventors: PERLMAN, Radia; 10 Huckleberry Lane, Acton, MA 01720-3731 (US). HANNA, Stephen; 3 Beverly Road, Bedford, MA 01730 (US).

(74) Agent: PARK, Richard; Suite 201, 508 2nd Street, Davis, CA 95616 (US).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

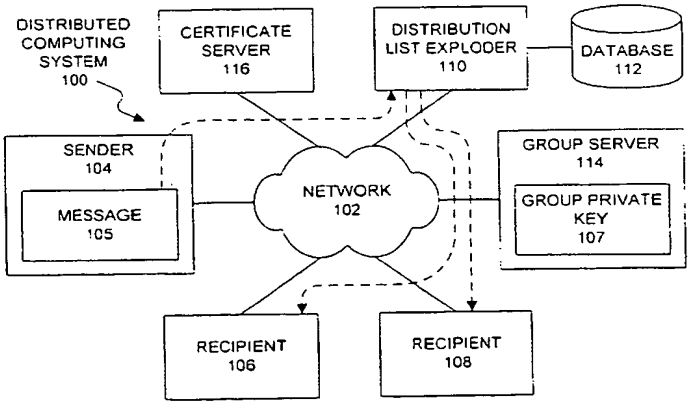
(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— with international search report

(88) Date of publication of the international search report:
21 February 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND APPARATUS FOR SENDING ENCRYPTED ELECTRONIC MAIL THROUGH A DISTRIBUTION LIST EXPLODER



(57) Abstract: One embodiment of the present invention provides a system for sending an encrypted message through a distribution list exploder in order to forward the encrypted message to recipients on a distribution list. The system operates by encrypting the message at a sender using a message key to form an encrypted message. The system also encrypts the message key with a group public key to form an encrypted message key. The group public key is associated with a group private key to form a public key-private key pair associated with a group of valid recipients for the message. Next, the system sends the encrypted message and the encrypted message key to the distribution list exploder, and the distribution list exploder forwards the encrypted message to a plurality of recipients specified in the distribution list. After receiving the encrypted message and the encrypted message key, the recipient decrypts the encrypted message key to restore the message key. Next, the recipient decrypts the encrypted message using the message key to restore the message. In a variation on the above embodiment, the recipient decrypts the encrypted message key by sending the encrypted message key from the recipient to a group server, which holds the group private key. The group server decrypts the encrypted message key using the group private key to restore the message key, and returns the message key to the recipient in a secure manner.

WO 01/41353 A3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/41995

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	HERFERT M: "SECURITY-ENHANCED MAILING LISTS" IEEE NETWORK,IEEE INC. NEW YORK,US, vol. 11, no. 3, 1 May 1997 (1997-05-01), pages 30-33, XP000689787 ISSN: 0890-8044	1-6, 10-19, 23-26, 30,31
Y	abstract page 30, right-hand column, line 8 - line 10 page 31, left-hand column, line 13 -right-hand column, line 20	7-9, 20-22, 27-29

-/--

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 June 2001	29/06/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Masche, C

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/41995

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	SERENELLI B ET AL: "SECURING ELECTRONIC MAIL SYSTEMS" SAN DIEGO, OCT. 11 - 14, 1992,NEW YORK, IEEE,US, vol. CONF. 11, 11 October 1992 (1992-10-11), pages 677-680, XP000346673 ISBN: 0-7803-0586-8	7-9, 20-22, 27-29
A	table I page 29.1.1, right-hand column, line 12 -page 29.1.2, right-hand column, line 9 page 29.1.4, left-hand column, line 11 -right-hand column, line 4	1-3,12, 14-16, 25,31
A	TSUTOMU MATSUMOTO ET AL: "ON THE KEY PREDISTRIBUTION SYSTEM: A PRACTICAL SOLUTION TO THE KEY DISTRIBUTION PROBLEM" PROCEEDINGS OF THE CONFERENCE ON THEORY AND APPLICATIONS OF CRYPTOGRAPHIC TECHNIQUES (CRYPTO),DE,BERLIN, SPRINGER, vol. CONF. 7, 1987, pages 185-193, XP000130202 abstract page 186, line 8 - line 40 page 189, line 1 - line 10	1,2,14, 15,25,31

N/A